Recent developments arising from the Gross-Zagier Theorem on singular moduli

Eyal Goren

McGill University

Montreal-Toronto Workshop in Number Theory, September 4-5, 2010

For $\tau \in \mathfrak{H}$ quadratic imaginary, the value $j(\tau)$ is called *singular modulus*. The basis of the theory of complex multiplication is that if $K = \mathbb{Q}(\tau)$and $\mathfrak{a} := \mathbb{Z} \oplus \mathbb{Z}\tau$ is an $\mathcal{O}_K$-module, then H_K, the Hilbert class field of K (the maximal abelian unramified extension of K), is equal to $K(j(\tau))$ and one knows the Galois action:

$$\left(\frac{\mathfrak{p},H}{K}\right) j(\mathfrak{a}) = j(\mathfrak{p}^{-1}\mathfrak{a}).$$

This has been generalized to any τ such that $K = \mathbb{Q}(\tau)$ is quadratic imaginary.

For $\tau \in \mathfrak{H}$ quadratic imaginary, the value $j(\tau)$ is called *singular modulus*. The basis of the theory of complex multiplication is that if $K = \mathbb{Q}(\tau)$and $\mathfrak{a} := \mathbb{Z} \oplus \mathbb{Z}\tau$ is an $\mathcal{O}_K$-module, then H_K, the Hilbert class field of K (the maximal abelian unramified extension of K), is equal to $K(j(\tau))$ and one knows the Galois action:

$$\left(\frac{\mathfrak{p}, H}{K}\right) j(\mathfrak{a}) = j(\mathfrak{p}^{-1}\mathfrak{a}).$$

This has been generalized to any τ such that $K = \mathbb{Q}(\tau)$ is quadratic imaginary.

The function j lives on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \cong \mathbb{A}^1_j(\mathbb{C})$, where $\mathbb{A}^1_j = \mathrm{Spec}(\mathbb{Z}[j])$, which is a coarse moduli scheme parameterizing elliptic curves up to isomorphism. Generalizations are of various types:

- Replace by $\Gamma\backslash\mathfrak{H}$, for $\Gamma = \Gamma_0(N), \Gamma_1(N), \Gamma(N)$.
- Replace by moduli schemes of abelian varieties with **P**olarization, **E**ndomorphisms, and **L**evel structure. These are called Shimura varieties of **PEL** type and are of the form

$$\Gamma\backslash G(\mathbb{R})/K,$$

where G is a reductive group over $\mathbb{Q}$, $X = G(\mathbb{R})/K$ is a hermitian symmetric space and K is a maximal compact subgroup of $G(\mathbb{R})$. For instance:

The function j lives on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \cong \mathbb{A}^1_j(\mathbb{C})$, where $\mathbb{A}^1_j = \mathrm{Spec}(\mathbb{Z}[j])$, which is a coarse moduli scheme parameterizing elliptic curves up to isomorphism. Generalizations are of various types:

- Replace by $\Gamma\backslash\mathfrak{H}$, for $\Gamma = \Gamma_0(N), \Gamma_1(N), \Gamma(N)$.
- Replace by moduli schemes of abelian varieties with **P**olarization, **E**ndomorphisms, and **L**evel structure. These are called Shimura varieties of **PEL** type and are of the form

$$\Gamma\backslash G(\mathbb{R})/K,$$

where G is a reductive group over $\mathbb{Q}$, $X = G(\mathbb{R})/K$ is a hermitian symmetric space and K is a maximal compact subgroup of $G(\mathbb{R})$. For instance:

The function j lives on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \cong \mathbb{A}^1_j(\mathbb{C})$, where $\mathbb{A}^1_j = \mathrm{Spec}(\mathbb{Z}[j])$, which is a coarse moduli scheme parameterizing elliptic curves up to isomorphism. Generalizations are of various types:

- Replace by $\Gamma\backslash\mathfrak{H}$, for $\Gamma = \Gamma_0(N), \Gamma_1(N), \Gamma(N)$.
- Replace by moduli schemes of abelian varieties with **P**olarization, **E**ndomorphisms, and **L**evel structure. These are called Shimura varieties of **PEL** type and are of the form

$$\Gamma\backslash G(\mathbb{R})/K,$$

where G is a reductive group over $\mathbb{Q}$, $X = G(\mathbb{R})/K$ is a hermitian symmetric space and K is a maximal compact subgroup of $G(\mathbb{R})$. For instance:

-
  - $G = \mathrm{Symp}_{2g}, \Gamma = \mathrm{Symp}_{2g}(\mathbb{Z})$ corresponds to principally polarized g-dimensional abelian varieties.
  - $G = \mathrm{Res}_{\mathrm{L}/\mathbb{Q}}\mathrm{GL}_2, \Gamma = \mathrm{GL}_2(\mathcal{O}_{\mathrm{L}})$ corresponds to (suitably) polarized g-dimensional abelian varieties with RM by $\mathcal{O}_L$.
- $G = U(n, m)$ corresponds to $n + m$-dimensional abelian varieties with an action of an imaginary quadratic field.

The singular moduli become the "special points" - the points in $X = G(\mathbb{R})/K$, whose stabilizer in G contains a maximal torus T, defined over $\mathbb{Q}$, such that $T(\mathbb{R})$ is compact. Shimura gave a general reciprocity law for the values $J(\tau)$, where τ is a special point on X and J is a "nice function". However, grosso modo, the nature of these numbers is poorly understood.

-
  - $G = \mathrm{Symp}_{2g}, \Gamma = \mathrm{Symp}_{2g}(\mathbb{Z})$ corresponds to principally polarized g-dimensional abelian varieties.
  - $G = \mathrm{Res}_{L/\mathbb{Q}}\mathrm{GL}_2, \Gamma = \mathrm{GL}_2(\mathcal{O}_L)$ corresponds to (suitably) polarized g-dimensional abelian varieties with RM by $\mathcal{O}_L$.
- $G = U(n, m)$ corresponds to $n + m$-dimensional abelian varieties with an action of an imaginary quadratic field.

The singular moduli become the “special points” - the points in $X = G(\mathbb{R})/K$, whose stabilizer in G contains a maximal torus T, defined over $\mathbb{Q}$, such that $T(\mathbb{R})$ is compact. Shimura gave a general reciprocity law for the values $J(\tau)$, where τ is a special point on X and J is a “nice function”. However, grosso modo, the nature of these numbers is poorly understood.

-
  - $G = \mathrm{Symp}_{2g}, \Gamma = \mathrm{Symp}_{2g}(\mathbb{Z})$ corresponds to principally polarized g-dimensional abelian varieties.
  - $G = \mathrm{Res}_{\mathrm{L}/\mathbb{Q}}\mathrm{GL}_2, \Gamma = \mathrm{GL}_2(\mathcal{O}_{\mathrm{L}})$ corresponds to (suitably) polarized g-dimensional abelian varieties with RM by $\mathcal{O}_L$.
- $G = U(n, m)$ corresponds to $n + m$-dimensional abelian varieties with an action of an imaginary quadratic field.

The singular moduli become the “special points” - the points in $X = G(\mathbb{R})/K$, whose stabilizer in G contains a maximal torus T, defined over $\mathbb{Q}$, such that $T(\mathbb{R})$ is compact. Shimura gave a general reciprocity law for the values $J(\tau)$, where τ is a special point on X and J is a “nice function”. However, grosso modo, the nature of these numbers is poorly understood.

-
  - $G = \mathrm{Symp}_{2g}, \Gamma = \mathrm{Symp}_{2g}(\mathbb{Z})$ corresponds to principally polarized g-dimensional abelian varieties.
  - $G = \mathrm{Res}_{\mathrm{L}/\mathbb{Q}}\mathrm{GL}_2, \Gamma = \mathrm{GL}_2(\mathcal{O}_{\mathrm{L}})$ corresponds to (suitably) polarized g-dimensional abelian varieties with RM by $\mathcal{O}_L$.
- $G = U(n, m)$ corresponds to $n + m$-dimensional abelian varieties with an action of an imaginary quadratic field.

The singular moduli become the "special points" - the points in $X = G(\mathbb{R})/K$, whose stabilizer in G contains a maximal torus T, defined over $\mathbb{Q}$, such that $T(\mathbb{R})$ is compact. Shimura gave a general reciprocity law for the values $J(\tau)$, where τ is a special point on X and J is a "nice function". However, grosso modo, the nature of these numbers is poorly understood.

-
  - $G = \mathrm{Symp}_{2g}, \Gamma = \mathrm{Symp}_{2g}(\mathbb{Z})$ corresponds to principally polarized g-dimensional abelian varieties.
  - $G = \mathrm{Res}_{\mathrm{L}/\mathbb{Q}}\mathrm{GL}_2, \Gamma = \mathrm{GL}_2(\mathcal{O}_{\mathrm{L}})$ corresponds to (suitably) polarized g-dimensional abelian varieties with RM by $\mathcal{O}_L$.
- $G = U(n, m)$ corresponds to $n + m$-dimensional abelian varieties with an action of an imaginary quadratic field.

The singular moduli become the “special points” - the points in $X = G(\mathbb{R})/K$, whose stabilizer in G contains a maximal torus T, defined over $\mathbb{Q}$, such that $T(\mathbb{R})$ is compact. Shimura gave a general reciprocity law for the values $J(\tau)$, where τ is a special point on X and J is a “nice function”. However, grosso modo, the nature of these numbers is poorly understood.

Deligne re-organized Shimura's work and included also spaces $X = G(\mathbb{R})/K$, coming from a reductive group G over $\mathbb{Q}$, for which there is no simple moduli interpretation. Notably:

$$X = \mathrm{SO}(2, n)/\mathrm{S}(\mathrm{O}(2) \times \mathrm{O}(n)).$$

These symmetric spaces can still be understood as moduli schemes of complex abelian varieties with given Hodge classes (in vector spaces constructed from their Betti cohomology), and the special points are defined as above. Their theory has been developing slowly over the last 20 years, where a big impetus, especially for $\mathrm{SO}(2, n)$ came from 2 sources:

Deligne re-organized Shimura's work and included also spaces $X = G(\mathbb{R})/K$, coming from a reductive group G over $\mathbb{Q}$, for which there is no simple moduli interpretation. Notably:

$$X = \mathrm{SO}(2, n)/\mathrm{S}(\mathrm{O}(2) \times \mathrm{O}(n)).$$

These symmetric spaces can still be understood as moduli schemes of complex abelian varieties with given Hodge classes (in vector spaces constructed from their Betti cohomology), and the special points are defined as above. Their theory has been developing slowly over the last 20 years, where a big impetus, especially for $\mathrm{SO}(2, n)$ came from 2 sources:

Deligne re-organized Shimura's work and included also spaces $X = G(\mathbb{R})/K$, coming from a reductive group G over $\mathbb{Q}$, for which there is no simple moduli interpretation. Notably:

$$X = \mathrm{SO}(2, n)/\mathrm{S}(\mathrm{O}(2) \times \mathrm{O}(n)).$$

These symmetric spaces can still be understood as moduli schemes of complex abelian varieties with given Hodge classes (in vector spaces constructed from their Betti cohomology), and the special points are defined as above. Their theory has been developing slowly over the last 20 years, where a big impetus, especially for $\mathrm{SO}(2, n)$ came from 2 sources:

A) The work of Borcherds allowed one to construct functions on X, starting from certain elliptic (vector-values) modular forms, a more accessible object. The special points are also accessible. Andrew Fiori has developed a theory for their classification.

Theorem ($-\epsilon$, Fiori, 2010)

Let (V, q) be a quadratic space (over k a number field) of dimension $2n$ or $2n+1$ and let (E, σ) be an étale algebra with involution over k of dimension $2n$. The algebraic group over k, O_q contains a torus of type (E, σ) if and only if:

1. *E^{ϕ} splits the even Clifford algebra C_q^0 for all reflex types ϕ of E.*
2. *If $\dim(V)$ is even then $\delta_{E/k} = (-1)^n D(q)$.*

A) The work of Borcherds allowed one to construct functions on X, starting from certain elliptic (vector-values) modular forms, a more accessible object. The special points are also accessible. Andrew Fiori has developed a theory for their classification.

Theorem ($-\epsilon$, Fiori, 2010)

Let (V, q) be a quadratic space (over k a number field) of dimension $2n$ or $2n+1$ and let (E, σ) be an étale algebra with involution over k of dimension $2n$. The algebraic group over k, O_q contains a torus of type (E, σ) if and only if:

1. *E^ϕ splits the even Clifford algebra C_q^0 for all reflex types ϕ of E.*
2. *If $\dim(V)$ is even then $\delta_{E/k} = (-1)^n D(q)$.*

B) The theory of rational canonical models, pioneered by Shimura and reformed by Deligne and Milne, has been extended by Vasiu (and, more recently, by Kisin) to a theory of integral models. One of the motivations being the study of the zeta function of these varieties as a test case for the Langlands conjectures.

The issue is the following: for $X = G(\mathbb{R})/K$ and a quotient $\Gamma\backslash X$, where G is a reductive group over $\mathbb{Q}$, one wants a canonical model defined over a number field $F(\Gamma)$. This was achieved by Shimura and Deligne.

In the theory of *integral* models one wants a model defined over $\mathcal{O}_{F(\Gamma)}[S^{-1}]$, where S - minimal as possible - is determined by group theoretic data associated with G. (E.g., for $\mathrm{SO}(2, n)$, S should be (at worst) the primes dividing the discriminant of the quadratic form, and perhaps the prime 2.)

B) The theory of rational canonical models, pioneered by Shimura and reformed by Deligne and Milne, has been extended by Vasiu (and, more recently, by Kisin) to a theory of integral models. One of the motivations being the study of the zeta function of these varieties as a test case for the Langlands conjectures.

The issue is the following: for $X = G(\mathbb{R})/K$ and a quotient $\Gamma\backslash X$, where G is a reductive group over $\mathbb{Q}$, one wants a canonical model defined over a number field $F(\Gamma)$. This was achieved by Shimura and Deligne.

In the theory of *integral* models one wants a model defined over $\mathcal{O}_{F(\Gamma)}[S^{-1}]$, where S - minimal as possible - is determined by group theoretic data associated with G. (E.g., for $\mathrm{SO}(2, n)$, S should be (at worst) the primes dividing the discriminant of the quadratic form, and perhaps the prime 2.)

B) The theory of rational canonical models, pioneered by Shimura and reformed by Deligne and Milne, has been extended by Vasiu (and, more recently, by Kisin) to a theory of integral models. One of the motivations being the study of the zeta function of these varieties as a test case for the Langlands conjectures.

The issue is the following: for $X = G(\mathbb{R})/K$ and a quotient $\Gamma\backslash X$, where G is a reductive group over $\mathbb{Q}$, one wants a canonical model defined over a number field $F(\Gamma)$. This was achieved by Shimura and Deligne.

In the theory of *integral* models one wants a model defined over $\mathcal{O}_{F(\Gamma)}[S^{-1}]$, where S - minimal as possible - is determined by group theoretic data associated with G. (E.g., for $\mathrm{SO}(2, n)$, S should be (at worst) the primes dividing the discriminant of the quadratic form, and perhaps the prime 2.)

The work of Gross-Zagier

It is a classical fact that $j(\tau)$ is an algebraic integer. In fact, if J is a function on a modular curve such that the polar part of its divisor is supported on the cusps then $J(\tau)$ is an algebraic integer for any quadratic imaginary τ. A natural question is thus,

What is the prime factorization of $j(\tau)$?

The curve $E_0 : y^2 = x^3 + 1$ has CM by $\mathbb{Z}[\omega]$, where ω is a primitive root of 1 and $j = 0$. It is parameterized by the point $\omega \in \mathfrak{H}$. We can rephrase our question as

What is the prime factorization of $j(\tau) - j(\omega)$?

And this question is very close to asking

What are the primes $\mathfrak{p}$ for which E_τ is isomorphic to E_0 modulo $\mathfrak{p}$?

The work of Gross-Zagier

It is a classical fact that $j(\tau)$ is an algebraic integer. In fact, if J is a function on a modular curve such that the polar part of its divisor is supported on the cusps then $J(\tau)$ is an algebraic integer for any quadratic imaginary τ. A natural question is thus,

What is the prime factorization of $j(\tau)$?

The curve $E_0 : y^2 = x^3 + 1$ has CM by $\mathbb{Z}[\omega]$, where ω is a primitive root of 1 and $j = 0$. It is parameterized by the point $\omega \in \mathfrak{H}$. We can rephrase our question as

What is the prime factorization of $j(\tau) - j(\omega)$?

And this question is very close to asking

What are the primes $\mathfrak{p}$ for which E_τ is isomorphic to E_0 modulo $\mathfrak{p}$?

The work of Gross-Zagier

It is a classical fact that $j(\tau)$ is an algebraic integer. In fact, if J is a function on a modular curve such that the polar part of its divisor is supported on the cusps then $J(\tau)$ is an algebraic integer for any quadratic imaginary τ. A natural question is thus,

What is the prime factorization of $j(\tau)$?

The curve $E_0 : y^2 = x^3 + 1$ has CM by $\mathbb{Z}[\omega]$, where ω is a primitive root of 1 and $j = 0$. It is parameterized by the point $\omega \in \mathfrak{H}$. We can rephrase our question as

What is the prime factorization of $j(\tau) - j(\omega)$?

And this question is very close to asking

What are the primes $\mathfrak{p}$ for which E_τ is isomorphic to E_0 modulo $\mathfrak{p}$?

The work of Gross-Zagier

It is a classical fact that $j(\tau)$ is an algebraic integer. In fact, if J is a function on a modular curve such that the polar part of its divisor is supported on the cusps then $J(\tau)$ is an algebraic integer for any quadratic imaginary τ. A natural question is thus,

What is the prime factorization of $j(\tau)$?

The curve $E_0 : y^2 = x^3 + 1$ has CM by $\mathbb{Z}[\omega]$, where ω is a primitive root of 1 and $j = 0$. It is parameterized by the point $\omega \in \mathfrak{H}$. We can rephrase our question as

What is the prime factorization of $j(\tau) - j(\omega)$?

And this question is very close to asking

What are the primes $\mathfrak{p}$ for which E_τ is isomorphic to E_0 modulo $\mathfrak{p}$?

The work of Gross-Zagier

It is a classical fact that $j(\tau)$ is an algebraic integer. In fact, if J is a function on a modular curve such that the polar part of its divisor is supported on the cusps then $J(\tau)$ is an algebraic integer for any quadratic imaginary τ. A natural question is thus,

What is the prime factorization of $j(\tau)$?

The curve $E_0 : y^2 = x^3 + 1$ has CM by $\mathbb{Z}[\omega]$, where ω is a primitive root of 1 and $j = 0$. It is parameterized by the point $\omega \in \mathfrak{H}$. We can rephrase our question as

What is the prime factorization of $j(\tau) - j(\omega)$?

And this question is very close to asking

What are the primes $\mathfrak{p}$ for which E_τ is isomorphic to E_0 modulo $\mathfrak{p}$?

One can make this connection more precise:

Lemma (Gross-Zagier)

Let j_i, $i = 1, 2$, be integral j-invariants in $W(\overline{\mathbb{F}}_p)$ with corresponding elliptic curves E_i with good reduction. Denote by $\mathrm{Isom}_n(E_1, E_2)$ the set of isomorphisms between the reduction of E_1 and E_2 modulo p^n, then:

$$\mathrm{val}_p(j_1 - j_2) = \frac{1}{2} \sum_{n \geq 1} \sharp\, \mathrm{Isom}_n(E_1, E_2).$$

Gross-Zagier on singular moduli

$K_i = \mathbb{Q}(\sqrt{d_i})$, $d_i < 0$ fund'l discriminant, $(d_1, d_2) = 1$, $w_i = \sharp\mathcal{O}_{K_i}^\times$.

$$J(d_1, d_2) := \prod_{[\tau_1],[\tau_2]} (j(\tau_1) - j(\tau_2))^{4/w_1 w_2}.$$

(τ_i is associated with K_i.)

Then:

$$J(d_1, d_2)^2 = \pm \prod_{x^2+4nn'=d_1 d_2} n^{\epsilon(n')}.$$

Here ϵ is multiplicative and $\epsilon(\ell)$ for a prime ℓ such that $\left(\frac{d_1 d_2}{\ell}\right) = -1$ is

$$= \begin{cases} \left(\frac{d_1}{\ell}\right) & \text{if } (d_1, \ell) = 1 \\ \left(\frac{d_2}{\ell}\right) & \text{if } (d_2, \ell) = 1. \end{cases}$$

Gross-Zagier on singular moduli

$K_i = \mathbb{Q}(\sqrt{d_i})$, $d_i < 0$ fund'l discriminant, $(d_1, d_2) = 1$, $w_i = \sharp\mathcal{O}_{K_i}^{\times}$.

$$J(d_1, d_2) := \prod_{[\tau_1],[\tau_2]} (j(\tau_1) - j(\tau_2))^{4/w_1 w_2}.$$

(τ_i is associated with K_i.)

Then:

$$J(d_1, d_2)^2 = \pm \prod_{x^2+4nn'=d_1 d_2} n^{\epsilon(n')}.$$

Here ϵ is multiplicative and $\epsilon(\ell)$ for a prime ℓ such that $\left(\frac{d_1 d_2}{\ell}\right) = -1$ is

$$= \begin{cases} \left(\frac{d_1}{\ell}\right) & \text{if } (d_1, \ell) = 1 \\ \left(\frac{d_2}{\ell}\right) & \text{if } (d_2, \ell) = 1. \end{cases}$$

Gross-Zagier on singular moduli

$K_i = \mathbb{Q}(\sqrt{d_i})$, $d_i < 0$ fund'l discriminant, $(d_1, d_2) = 1$, $w_i = \sharp\mathcal{O}_{K_i}^\times$.

$$J(d_1, d_2) := \prod_{[\tau_1],[\tau_2]} (j(\tau_1) - j(\tau_2))^{4/w_1 w_2}.$$

(τ_i is associated with K_i.)

Then:

$$J(d_1, d_2)^2 = \pm \prod_{x^2+4nn'=d_1 d_2} n^{\epsilon(n')}.$$

Here ϵ is multiplicative and $\epsilon(\ell)$ for a prime ℓ such that $\left(\frac{d_1 d_2}{\ell}\right) = -1$ is

$$= \begin{cases} \left(\frac{d_1}{\ell}\right) & \text{if } (d_1, \ell) = 1 \\ \left(\frac{d_2}{\ell}\right) & \text{if } (d_2, \ell) = 1. \end{cases}$$

Example

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -2^{18}3^3 5^3 23^3 29^3.$$

$$j\left(\frac{1+\sqrt{-163}}{2}\right) - 1728 = -2^6 3^6 7^2 11^2 19^2 127^2 163.$$

$(0 = j(e^{2\pi i/3}), 1728 = j(i).)$

A better version of Gross-Zagier, though less elegant, is

$$\mathrm{ord}_\ell(J(d_1, d_2)) = \frac{1}{2}\sum_{x\in\mathbb{Z}}\sum_{n\geq 1}\delta(x)R\left(\frac{d_1 d_2 - x^2}{4\ell^n}\right),$$

where $R(m)$ is the number of ideals of $\mathcal{O}_K$ of norm m and $\delta(x) = 1$, unless x is divisible by ℓ, in which case it is 2.

Example

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -2^{18}3^35^323^329^3.$$

$$j\left(\frac{1+\sqrt{-163}}{2}\right) - 1728 = -2^63^67^211^219^2127^2163.$$

$(0 = j(e^{2\pi i/3}), 1728 = j(i).)$

A better version of Gross-Zagier, though less elegant, is

$$\mathrm{ord}_\ell(J(d_1, d_2)) = \frac{1}{2}\sum_{x\in\mathbb{Z}}\sum_{n\geq 1}\delta(x)R\left(\frac{d_1d_2 - x^2}{4\ell^n}\right),$$

where $R(m)$ is the number of ideals of $\mathcal{O}_K$ of norm m and $\delta(x) = 1$, unless x is divisible by ℓ, in which case it is 2.

Gross-Zagier's strategy - algebraic proof

For $E/\overline{\mathbb{F}}_p$, $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}, K, B_{p,\infty}$.

Key point: We must be in the last case. Use K to present $B_{p,\infty}$ and then study optimal embeddings into these maximal orders containing $\mathcal{O}_K$.

Key ingredients:

1) Explicit description of all the maximal orders into which $\mathcal{O}_K$ embeds. (GZ's proof assumes K has prime discriminant. Dorman gave a more general proof and had to extend this result.)

Gross-Zagier's strategy - algebraic proof

For $E/\overline{\mathbb{F}}_p$, $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}, K, B_{p,\infty}$.

Key point: We must be in the last case. Use K to present $B_{p,\infty}$ and then study optimal embeddings into these maximal orders containing $\mathcal{O}_K$.

Key ingredients:

1) Explicit description of all the maximal orders into which $\mathcal{O}_K$ embeds. (GZ's proof assumes K has prime discriminant. Dorman gave a more general proof and had to extend this result.)

Gross-Zagier's strategy - algebraic proof

For $E/\overline{\mathbb{F}}_p$, $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}, K, B_{p,\infty}$.

Key point: We must be in the last case. Use K to present $B_{p,\infty}$ and then study optimal embeddings into these maximal orders containing $\mathcal{O}_K$.

Key ingredients:

1) Explicit description of all the maximal orders into which $\mathcal{O}_K$ embeds. (GZ's proof assumes K has prime discriminant. Dorman gave a more general proof and had to extend this result.)

Gross-Zagier's strategy - algebraic proof

For $E/\overline{\mathbb{F}}_p$, $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}, K, B_{p,\infty}$.

Key point: We must be in the last case. Use K to present $B_{p,\infty}$ and then study optimal embeddings into these maximal orders containing $\mathcal{O}_K$.

Key ingredients:

1) Explicit description of all the maximal orders into which $\mathcal{O}_K$ embeds. (GZ's proof assumes K has prime discriminant. Dorman gave a more general proof and had to extend this result.)

2) Calculating

$$\mathrm{End}(E/W_n(\overline{\mathbb{F}}_p)) = \mathcal{O}_K + p^{n-1}R,$$

where $R = \mathrm{End}(E \pmod p)$.

(Completed by Gross in a later paper that uses strongly that the formal group is 1-dim'l.)

3) Arithmetic intersection formula for $v(j_1 - j_2)$.

$$v(j_1 - j_2) = \frac{1}{2}\sum_{n\geq 1} \sharp \mathrm{Isom}_n(E_1, E_2).$$

This connects the arithmetic of j-invariants to arithmetic geometry of elliptic curves.

2) Calculating

$$\mathrm{End}(E/W_n(\overline{\mathbb{F}}_p)) = \mathcal{O}_K + p^{n-1}R,$$

where $R = \mathrm{End}(E \pmod p)$.

(Completed by Gross in a later paper that uses strongly that the formal group is 1-dim'l.)

3) Arithmetic intersection formula for $v(j_1 - j_2)$.

$$v(j_1 - j_2) = \frac{1}{2}\sum_{n\geq 1} \sharp\mathrm{Isom}_n(E_1, E_2).$$

This connects the arithmetic of j-invariants to arithmetic geometry of elliptic curves.

From the point of view of the lemma on $v(j_1 - j_2)$, the theorem can be viewed as calculating an arithmetic intersection number (between the points j_1, j_2) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$, or, from Arakelov theory perspective, the finite part of it. Equivalently, we may view it as calculating an arithmetic intersection number (between the point (j_1, j_2) and the diagonal) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. The diagonal is the divisor of $j(\tau_1) - j(\tau_2)$, which happens to be a Borcherds lift. The function is also a Green function of that divisor, so in the sense of Arakelov theory, the intersection number is 0. One concludes that the finite intersection number can be calculated via the archimedean contribution. This is the point of view taken by Bruinier and Yang, employing that the Brocherds lift is always a Green function for its divisor.

From the point of view of the lemma on $v(j_1 - j_2)$, the theorem can be viewed as calculating an arithmetic intersection number (between the points j_1, j_2) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$, or, from Arakelov theory perspective, the finite part of it. Equivalently, we may view it as calculating an arithmetic intersection number (between the point (j_1, j_2) and the diagonal) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. The diagonal is the divisor of $j(\tau_1) - j(\tau_2)$, which happens to be a Borcherds lift. The function is also a Green function of that divisor, so in the sense of Arakelov theory, the intersection number is 0. One concludes that the finite intersection number can be calculated via the archimedean contribution. This is the point of view taken by Bruinier and Yang, employing that the Brocherds lift is always a Green function for its divisor.

From the point of view of the lemma on $v(j_1 - j_2)$, the theorem can be viewed as calculating an arithmetic intersection number (between the points j_1, j_2) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$, or, from Arakelov theory perspective, the finite part of it. Equivalently, we may view it as calculating an arithmetic intersection number (between the point (j_1, j_2) and the diagonal) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. The diagonal is the divisor of $j(\tau_1) - j(\tau_2)$, which happens to be a Borcherds lift. The function is also a Green function of that divisor, so in the sense of Arakelov theory, the intersection number is 0. One concludes that the finite intersection number can be calculated via the archimedean contribution. This is the point of view taken by Bruinier and Yang, employing that the Brocherds lift is always a Green function for its divisor.

From the point of view of the lemma on $v(j_1 - j_2)$, the theorem can be viewed as calculating an arithmetic intersection number (between the points j_1, j_2) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$, or, from Arakelov theory perspective, the finite part of it. Equivalently, we may view it as calculating an arithmetic intersection number (between the point (j_1, j_2) and the diagonal) on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. The diagonal is the divisor of $j(\tau_1) - j(\tau_2)$, which happens to be a Borcherds lift. The function is also a Green function of that divisor, so in the sense of Arakelov theory, the intersection number is 0. One concludes that the finite intersection number can be calculated via the archimedean contribution. This is the point of view taken by Bruinier and Yang, employing that the Brocherds lift is always a Green function for its divisor.

This point of view suggests further study:

- What about points on Shimura varieties? Elkies, Schofer, Errthum, Voight ...
- What about other symmetric functions, e.g., traces of singular moduli? Zagier, Ono (with Ahlgren, Jenkins, Bringmann, Rouse), Bruinier, Funke ....
- Can one refine the result of Gross-Zagier? Can one determine the factorization of $j(\tau_1) - j(\tau_2)$ and not just its norm?
- What about higher dimensional varieties? Bruinier, Kudla, Rapoport, Yang and in geometric setting Hirzebruch-Zagier, van der Geer, Cogdell, Kudla, Milson, Getz-Goresky, Terstiege... In Arakelov setting also Burgos, Kramer, Hoermann ....

This point of view suggests further study:

- What about points on Shimura varieties? Elkies, Schofer, Errthum, Voight ...
- What about other symmetric functions, e.g., traces of singular moduli? Zagier, Ono (with Ahlgren, Jenkins, Bringmann, Rouse), Bruinier, Funke ....
- Can one refine the result of Gross-Zagier? Can one determine the factorization of $j(\tau_1) - j(\tau_2)$ and not just its norm?
- What about higher dimensional varieties? Bruinier, Kudla, Rapoport, Yang and in geometric setting Hirzebruch-Zagier, van der Geer, Cogdell, Kudla, Milson, Getz-Goresky, Terstiege... In Arakelov setting also Burgos, Kramer, Hoermann ....

This point of view suggests further study:

- What about points on Shimura varieties? Elkies, Schofer, Errthum, Voight ...
- What about other symmetric functions, e.g., traces of singular moduli? Zagier, Ono (with Ahlgren, Jenkins, Bringmann, Rouse), Bruinier, Funke ....
- Can one refine the result of Gross-Zagier? Can one determine the factorization of $j(\tau_1) - j(\tau_2)$ and not just its norm?
- What about higher dimensional varieties? Bruinier, Kudla, Rapoport, Yang and in geometric setting Hirzebruch-Zagier, van der Geer, Cogdell, Kudla, Milson, Getz-Goresky, Terstiege... In Arakelov setting also Burgos, Kramer, Hoermann ....

This point of view suggests further study:

- What about points on Shimura varieties? Elkies, Schofer, Errthum, Voight ...
- What about other symmetric functions, e.g., traces of singular moduli? Zagier, Ono (with Ahlgren, Jenkins, Bringmann, Rouse), Bruinier, Funke ....
- Can one refine the result of Gross-Zagier? Can one determine the factorization of $j(\tau_1) - j(\tau_2)$ and not just its norm?
- What about higher dimensional varieties? Bruinier, Kudla, Rapoport, Yang and in geometric setting Hirzebruch-Zagier, van der Geer, Cogdell, Kudla, Milson, Getz-Goresky, Terstiege... In Arakelov setting also Burgos, Kramer, Hoermann ....

This point of view suggests further study:

- What about points on Shimura varieties? Elkies, Schofer, Errthum, Voight ...
- What about other symmetric functions, e.g., traces of singular moduli? Zagier, Ono (with Ahlgren, Jenkins, Bringmann, Rouse), Bruinier, Funke ....
- Can one refine the result of Gross-Zagier? Can one determine the factorization of $j(\tau_1) - j(\tau_2)$ and not just its norm?
- What about higher dimensional varieties? Bruinier, Kudla, Rapoport, Yang and in geometric setting Hirzebruch-Zagier, van der Geer, Cogdell, Kudla, Milson, Getz-Goresky, Terstiege... In Arakelov setting also Burgos, Kramer, Hoermann ....

The work of Schofer, Bruinier-Yang, Bruinier-Kudla-Yang

The setting is the following:

Let $L \subseteq (V, q)$ a lattice of signature $(2, n)$, where $n \geq 0$.

Let f be a vector-valued weakly holomorphic elliptic modular form in $\mathrm{Mod}^!(\mathbb{C}[L'/L], 1 - n/2, \rho_L)$ whose Fourier expansion is

$$\sum_{\mu \in L'/L} \sum_{n \in q(\mu)+\mathbb{Z}} c(\mu, n) q^n \mathbf{e}_\mu .$$

Assume that $c(\mu, n) \in \mathbb{Z}$ for $n \leq 0$.

Let $\Psi(f)$ be the Borcherds lift of f. It is a modular form on $SO(2, n)$, of weight $c(0,0)/2$ and level $\Gamma(L) = \left\{ M \in SO_q(\mathbb{Z}) : M|_{L'/L} = \mathrm{Id} \right\}$.

Recall that $\Psi(f)$ is defined on the Grassmannian X of positive definite planes of V.

The work of Schofer, Bruinier-Yang, Bruinier-Kudla-Yang

The setting is the following:

Let $L \subseteq (V, q)$ a lattice of signature $(2, n)$, where $n \geq 0$.

Let f be a vector-valued weakly holomorphic elliptic modular form in $\mathrm{Mod}^!(\mathbb{C}[L'/L], 1 - n/2, \rho_L)$ whose Fourier expansion is

$$\sum_{\mu \in L'/L} \sum_{n \in q(\mu)+\mathbb{Z}} c(\mu, n) q^n \mathbf{e}_\mu.$$

Assume that $c(\mu, n) \in \mathbb{Z}$ for $n \leq 0$.

Let $\Psi(f)$ be the Borcherds lift of f. It is a modular form on $SO(2, n)$, of weight $c(0, 0)/2$ and level $\Gamma(L) = \{M \in SO_q(\mathbb{Z}) : M|_{L'/L} = \mathrm{Id}\}$.

Recall that $\Psi(f)$ is defined on the Grassmannian X of positive definite planes of V.

The work of Schofer, Bruinier-Yang, Bruinier-Kudla-Yang

The setting is the following:

Let $L \subseteq (V, q)$ a lattice of signature $(2, n)$, where $n \geq 0$.

Let f be a vector-valued weakly holomorphic elliptic modular form in $\mathrm{Mod}^!(\mathbb{C}[L'/L], 1 - n/2, \rho_L)$ whose Fourier expansion is

$$\sum_{\mu \in L'/L} \sum_{n \in q(\mu)+\mathbb{Z}} c(\mu, n) q^n \mathbf{e}_\mu.$$

Assume that $c(\mu, n) \in \mathbb{Z}$ for $n \leq 0$.

Let $\Psi(f)$ be the Borcherds lift of f. It is a modular form on $SO(2, n)$, of weight $c(0, 0)/2$ and level $\Gamma(L) = \{M \in SO_q(\mathbb{Z}) : M|_{L'/L} = \mathrm{Id}\}$.

Recall that $\Psi(f)$ is defined on the Grassmannian X of positive definite planes of V.

The work of Schofer, Bruinier-Yang, Bruinier-Kudla-Yang

The setting is the following:

Let $L \subseteq (V, q)$ a lattice of signature $(2, n)$, where $n \geq 0$.

Let f be a vector-valued weakly holomorphic elliptic modular form in $\mathrm{Mod}^!(\mathbb{C}[L'/L], 1 - n/2, \rho_L)$ whose Fourier expansion is

$$\sum_{\mu \in L'/L} \sum_{n \in q(\mu)+\mathbb{Z}} c(\mu, n) q^n \mathbf{e}_\mu.$$

Assume that $c(\mu, n) \in \mathbb{Z}$ for $n \leq 0$.

Let $\Psi(f)$ be the Borcherds lift of f. It is a modular form on $SO(2, n)$, of weight $c(0,0)/2$ and level $\Gamma(L) = \{M \in SO_q(\mathbb{Z}) : M|_{L'/L} = \mathrm{Id}\}$.

Recall that $\Psi(f)$ is defined on the Grassmannian X of positive definite planes of V.

Let $\lambda \in V$ be such that $q(\lambda) < 0$. Then $\lambda^\perp$ denotes all the points in X that are perpendicular to Λ. It is a divisor, naturally isomorphic to a symmetric variety of type $SO(2, n-1)$.

Define for $\mu \in L'/L$, $m < 0$.

$$H(\mu, \lambda) = \bigcup_{\lambda \in \mu + L, q(\lambda) = m} \lambda^\perp.$$

It is a locally finite divisor on X and its quotient on $\Gamma(L)\backslash X$ is an algebraic divisor $Z(\mu, m)$.

The divisor of $\Psi(f)$ is

$$\sum_{\mu, m<0} c(\mu, m) Z(\mu, m).$$

Given a CM cycle (more on that below) C on $\Gamma(L)\backslash X$, one wants to study

$$\Psi(f)(C) = \prod_{c \in C} \Psi(f)(c).$$

Let $\lambda \in V$ be such that $q(\lambda) < 0$. Then $\lambda^\perp$ denotes all the points in X that are perpendicular to Λ. It is a divisor, naturally isomorphic to a symmetric variety of type $SO(2, n-1)$.

Define for $\mu \in L'/L$, $m < 0$.

$$H(\mu, \lambda) = \bigcup_{\lambda \in \mu + L, q(\lambda) = m} \lambda^\perp.$$

It is a locally finite divisor on X and its quotient on $\Gamma(L)\backslash X$ is an algebraic divisor $Z(\mu, m)$.

The divisor of $\Psi(f)$ is

$$\sum_{\mu, m<0} c(\mu, m) Z(\mu, m).$$

Given a CM cycle (more on that below) C on $\Gamma(L)\backslash X$, one wants to study

$$\Psi(f)(C) = \prod_{c \in C} \Psi(f)(c).$$

Let $\lambda \in V$ be such that $q(\lambda) < 0$. Then $\lambda^\perp$ denotes all the points in X that are perpendicular to Λ. It is a divisor, naturally isomorphic to a symmetric variety of type $SO(2, n-1)$.

Define for $\mu \in L'/L$, $m < 0$.

$$H(\mu, \lambda) = \bigcup_{\lambda \in \mu + L, q(\lambda) = m} \lambda^\perp.$$

It is a locally finite divisor on X and its quotient on $\Gamma(L)\backslash X$ is an algebraic divisor $Z(\mu, m)$.

The divisor of $\Psi(f)$ is

$$\sum_{\mu, m<0} c(\mu, m) Z(\mu, m).$$

Given a CM cycle (more on that below) C on $\Gamma(L)\backslash X$, one wants to study

$$\Psi(f)(C) = \prod_{c \in C} \Psi(f)(c).$$

Let $\lambda \in V$ be such that $q(\lambda) < 0$. Then $\lambda^\perp$ denotes all the points in X that are perpendicular to Λ. It is a divisor, naturally isomorphic to a symmetric variety of type $SO(2, n-1)$.

Define for $\mu \in L'/L$, $m < 0$.

$$H(\mu, \lambda) = \bigcup_{\lambda \in \mu + L, q(\lambda) = m} \lambda^\perp.$$

It is a locally finite divisor on X and its quotient on $\Gamma(L)\backslash X$ is an algebraic divisor $Z(\mu, m)$.

The divisor of $\Psi(f)$ is

$$\sum_{\mu, m<0} c(\mu, m) Z(\mu, m).$$

Given a CM cycle (more on that below) C on $\Gamma(L)\backslash X$, one wants to study

$$\Psi(f)(C) = \prod_{c \in C} \Psi(f)(c).$$

Example

Let L be a real quadratic algebra over $\mathbb{Q}$, with involution $\lambda \mapsto \lambda'$. So, L is either a quadratic real field, or $\mathbb{Q} \oplus \mathbb{Q}$ with $(a, b)' = (b, a)$. Let

$$V = \{A \in M_2(\mathcal{O}_L) :\ {}^tA = A'\} \supset \Lambda = \left\{ \begin{pmatrix} a & \lambda \\ \lambda' & d \end{pmatrix} : a, d \in \mathbb{Z}, \lambda \in \mathcal{O}_L \right\}.$$

We endow V with the quadratic form $q(M) = \det(M)$. It has signature $(2, 2)$ and the bilinear form is $\langle A, B \rangle = \mathrm{Tr}(A \cdot adj(B))$. The group $\mathbf{SL}_2(\mathcal{O}_L)$ acts on V by

$$\gamma * A = \gamma' \cdot A \cdot^t \gamma.$$

This gives an isomorphism $\mathrm{PSL}_2(\mathcal{O}_L) \cong SO_q(\mathbb{Z})$.

Example

Let L be a real quadratic algebra over $\mathbb{Q}$, with involution $\lambda \mapsto \lambda'$. So, L is either a quadratic real field, or $\mathbb{Q} \oplus \mathbb{Q}$ with $(a, b)' = (b, a)$. Let

$$V = \{A \in M_2(\mathcal{O}_L) : \ {}^tA = A'\} \supset \Lambda = \left\{ \begin{pmatrix} a & \lambda \\ \lambda' & d \end{pmatrix} : a, d \in \mathbb{Z}, \lambda \in \mathcal{O}_L \right\}.$$

We endow V with the quadratic form $q(M) = \det(M)$. It has signature $(2, 2)$ and the bilinear form is $\langle A, B \rangle = \mathrm{Tr}(A \cdot adj(B))$.
The group $\mathbf{SL}_2(\mathcal{O}_L)$ acts on V by

$$\gamma * A = \gamma' \cdot A \cdot^t \gamma.$$

This gives an isomorphism $\mathrm{PSL}_2(\mathcal{O}_L) \cong SO_q(\mathbb{Z})$.

Example

Let L be a real quadratic algebra over $\mathbb{Q}$, with involution $\lambda \mapsto \lambda'$. So, L is either a quadratic real field, or $\mathbb{Q} \oplus \mathbb{Q}$ with $(a, b)' = (b, a)$. Let

$$V = \{A \in M_2(\mathcal{O}_L) : \ {}^tA = A'\} \supset \Lambda = \left\{ \begin{pmatrix} a & \lambda \\ \lambda' & d \end{pmatrix} : a, d \in \mathbb{Z}, \lambda \in \mathcal{O}_L \right\}.$$

We endow V with the quadratic form $q(M) = \det(M)$. It has signature $(2, 2)$ and the bilinear form is $\langle A, B\rangle = \mathrm{Tr}(A \cdot adj(B))$. The group $\mathbf{SL}_2(\mathcal{O}_L)$ acts on V by

$$\gamma * A = \gamma' \cdot A \cdot^t \gamma.$$

This gives an isomorphism $\mathrm{PSL}_2(\mathcal{O}_L) \cong SO_q(\mathbb{Z})$.

We have $\Lambda'/\Lambda = D_L^{-1}/\mathcal{O}_L \cong \mathbb{Z}/d_L\mathbb{Z}$, and so for $L = \mathbb{Q} \oplus \mathbb{Q}$ the lattice Λ is unimodular.

We have, $\sum_\mu Z(\mu, m) = T_m$, the Hirzebruch-Zagier cycle of index m, and for $L = \mathbb{Q} \oplus \mathbb{Q}$ it is the Hecke correspondence of level m.

We have $\Lambda'/\Lambda = D_L^{-1}/\mathcal{O}_L \cong \mathbb{Z}/d_L\mathbb{Z}$, and so for $L = \mathbb{Q} \oplus \mathbb{Q}$ the lattice Λ is unimodular.

We have, $\sum_\mu Z(\mu, m) = T_m$, the Hirzebruch-Zagier cycle of index m, and for $L = \mathbb{Q} \oplus \mathbb{Q}$ it is the Hecke correspondence of level m.

Continuing our example, the input space for the Borcherds lift are modular forms of weight 0, i.e., vector-valued functions with values in $\mathbb{C}[\mathbb{Z}/d_L\mathbb{Z}]$. These can be related to Jacobi forms.

In the example of $L = \mathbb{Q} \oplus \mathbb{Q}$ the input space is just modular functions with poles at $i\infty$. Namely, elements of $\mathbb{C}[j]$. The Borcherds lift of

$$j(q) - 744 = \frac{1}{q} + 196884q + \ldots\ldots$$

is a modular function on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ that vanishes along the diagonal, and, as suspected, is equal to $j(\tau_1) - j(\tau_2)$.

Continuing our example, the input space for the Borcherds lift are modular forms of weight 0, i.e., vector-valued functions with values in $\mathbb{C}[\mathbb{Z}/d_L\mathbb{Z}]$. These can be related to Jacobi forms.

In the example of $L = \mathbb{Q} \oplus \mathbb{Q}$ the input space is just modular functions with poles at $i\infty$. Namely, elements of $\mathbb{C}[j]$. The Borcherds lift of

$$j(q) - 744 = \frac{1}{q} + 196884q + \ldots \ldots$$

is a modular function on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ that vanishes along the diagonal, and, as suspected, is equal to $j(\tau_1) - j(\tau_2)$.

Continuing our example, the input space for the Borcherds lift are modular forms of weight 0, i.e., vector-valued functions with values in $\mathbb{C}[\mathbb{Z}/d_L\mathbb{Z}]$. These can be related to Jacobi forms.

In the example of $L = \mathbb{Q} \oplus \mathbb{Q}$ the input space is just modular functions with poles at $i\infty$. Namely, elements of $\mathbb{C}[j]$. The Borcherds lift of

$$j(q) - 744 = \frac{1}{q} + 196884q + \ldots\ldots$$

is a modular function on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ that vanishes along the diagonal, and, as suspected, is equal to $j(\tau_1) - j(\tau_2)$.

“Big” CM points on $SO(2,2)$

In their paper (Inventiones 2006) Bruinier and Yang obtain the following result for a function $\Psi(f)$ on $\mathbf{SL}_2(\mathcal{O}_L)\backslash\mathfrak{H}^2$ that is a Borcherds lift.

Theorem

Let C be the CM cycle associated to a primitive CM field K of degree 4, viewed on $\mathbf{SL}_2(\mathcal{O}_L)\backslash\mathfrak{H}^2$, where $L = K^+$. Assume that f has divisor $\sum_{m>0} \tilde{c}(-m)T_m$. Then,

$$\log|\Psi(f)(C)| = \frac{w_{K^*}}{4}\sum_{m\geq 0}\tilde{c}(-m)b_m.$$

$K^+ = \mathbb{Q}(\sqrt{p})$, where $p \equiv 1 \pmod 4$ is a prime and d_{K/K^+} is a prime ideal of residue degree 1 over a prime q of $\mathbb{Q}$ also $\equiv 1 \pmod 4$. K^* is the reflex field.

"Big" CM points on $SO(2,2)$

In their paper (Inventiones 2006) Bruinier and Yang obtain the following result for a function $\Psi(f)$ on $\mathbf{SL}_2(\mathcal{O}_L)\backslash\mathfrak{H}^2$ that is a Borcherds lift.

Theorem

Let C be the CM cycle associated to a primitive CM field K of degree 4, viewed on $\mathbf{SL}_2(\mathcal{O}_L)\backslash\mathfrak{H}^2$, where $L = K^+$. Assume that f has divisor $\sum_{m>0} \tilde{c}(-m)T_m$. Then,

$$\log|\Psi(f)(C)| = \frac{w_{K^*}}{4}\sum_{m\geq 0}\tilde{c}(-m)b_m.$$

$K^+ = \mathbb{Q}(\sqrt{p})$, where $p \equiv 1 \pmod 4$ is a prime and d_{K/K^+} is a prime ideal of residue degree 1 over a prime q of $\mathbb{Q}$ also $\equiv 1 \pmod 4$. K^* is the reflex field.

"Big" CM points on $SO(2,2)$

In their paper (Inventiones 2006) Bruinier and Yang obtain the following result for a function $\Psi(f)$ on $\mathbf{SL}_2(\mathcal{O}_L)\backslash\mathfrak{H}^2$ that is a Borcherds lift.

Theorem

Let C be the CM cycle associated to a primitive CM field K of degree 4, viewed on $\mathbf{SL}_2(\mathcal{O}_L)\backslash\mathfrak{H}^2$, where $L = K^+$. Assume that f has divisor $\sum_{m>0} \tilde{c}(-m)T_m$. Then,

$$\log|\Psi(f)(C)| = \frac{w_{K^*}}{4}\sum_{m\geq 0}\tilde{c}(-m)b_m.$$

$K^+ = \mathbb{Q}(\sqrt{p})$, where $p \equiv 1 \pmod 4$ is a prime and d_{K/K^+} is a prime ideal of residue degree 1 over a prime q of $\mathbb{Q}$ also $\equiv 1 \pmod 4$. K^* is the reflex field.

$$b_m = \sum_{\substack{t=\frac{n+m\sqrt{q}}{2p}\in d_{K^*/K^{*,+}}^{-1} \\ |n|<m\sqrt{q}}} B_t,$$

where,

$$B_t = \sum_{\ell\subset\mathcal{O}_{K^{*,+}},\ prime\ ideal} B_t(\ell),$$

and

$$B_t(\ell) = \begin{cases} 0 & \ell \text{ splits in } K^* \\ (ord_\ell t + 1)\rho(t d_{K^*/K^{*,+}}\ell^{-1}) \log|\ell| & else, \end{cases}$$

where,

$$\rho(\mathfrak{a}) = \sharp\left\{A \subseteq \mathcal{O}_{K^*} : N_{K^*/K^{*,+}} A = \mathfrak{a}\right\}.$$

As a result, they have formulated the conjecture that

$$T_m \cdot CM(K) = \frac{w_{K^*}}{4w_K} b_m.$$

"Small" CM points

In his paper (Crelle 2009), Schofer deals with small CM points, coming from quadratic imaginary fields, but "living" on a Shimura variety associated to a vector space of signature $(2, n)$. (His work was generalized by Bruinier and Yang in a subsequent work.) His theorem is the following:

Theorem

There exist explicit constants $\kappa(\mu, m)$ such that

$$-\sum_{z \in CM(K)} \log \|\Psi(f)(z)\| = \frac{1}{vol(K_P)} \sum_{\mu} \sum_{m \geq 0} c(\mu, -m)\kappa(\mu, m).$$

(Where $\|\cdot\|$ denotes the Peterson norm.)

The CM cycle comes from a splitting of $V = P \oplus U$, where P is positive definite and rational vector space of dimension 2 (one assume such a splitting exists). As such, P is essentially a quadratic imaginary field with its norm form. This gives us a point on X and the CM cycle is somehow constructed from this point. K_P is essentially $K \cap SO(P)$.

Based on such results, Bruinier and Yang had conjectured a formula for the finite part of the arithmetic intersection number $CM(K)_{\bullet}Z(\mu, m)$. It should be stressed that the constants $\kappa(\mu, m)$ are hard to understand.

The CM cycle comes from a splitting of $V = P \oplus U$, where P is positive definite and rational vector space of dimension 2 (one assume such a splitting exists). As such, P is essentially a quadratic imaginary field with its norm form. This gives us a point on X and the CM cycle is somehow constructed from this point. K_P is essentially $K \cap SO(P)$.

Based on such results, Bruinier and Yang had conjectured a formula for the finite part of the arithmetic intersection number $CM(K)_{\bullet}Z(\mu, m)$. It should be stressed that the constants $\kappa(\mu, m)$ are hard to understand.

"Big" CM points on $SO(2,n)$

In a very recent preprint, Bruinier-Kudla-Yang were able to generalize Schofer's methods to obtain such a result for CM cycles coming from primitive CM fields that produce special points on X - "the really interesting case". Based on that they have made a conjecture about $CM(K)_\bullet Z(\mu, m)$, which is wide open. However, their conjecture should, in principle, yield a bound on the largest prime that can appear in $CM(K)_\bullet Z(\mu, m)$ given K, μ, m. Farbizio Andreatta and me are trying to prove such a bound from a moduli theoretic point of view, attempting to generalize a very special case worked out by Goren-Lauter (Annales Fourier Inst. 2007).

"Big" CM points on $SO(2, n)$

In a very recent preprint, Bruinier-Kudla-Yang were able to generalize Schofer's methods to obtain such a result for CM cycles coming from primitive CM fields that produce special points on X - "the really interesting case". Based on that they have made a conjecture about $CM(K)_{\bullet}Z(\mu, m)$, which is wide open. However, their conjecture should, in principle, yield a bound on the largest prime that can appear in $CM(K)_{\bullet}Z(\mu, m)$ given K, μ, m. Farbizio Andreatta and me are trying to prove such a bound from a moduli theoretic point of view, attempting to generalize a very special case worked out by Goren-Lauter (Annales Fourier Inst. 2007).

"Big" CM points on $SO(2, n)$

In a very recent preprint, Bruinier-Kudla-Yang were able to generalize Schofer's methods to obtain such a result for CM cycles coming from primitive CM fields that produce special points on X - "the really interesting case". Based on that they have made a conjecture about $CM(K)_\bullet Z(\mu, m)$, which is wide open. However, their conjecture should, in principle, yield a bound on the largest prime that can appear in $CM(K)_\bullet Z(\mu, m)$ given K, μ, m. Farbizio Andreatta and me are trying to prove such a bound from a moduli theoretic point of view, attempting to generalize a very special case worked out by Goren-Lauter (Annales Fourier Inst. 2007).

A different generalization of Gross-Zagier

Let L be a totally real field, $[L:\mathbb{Q}] = g$, $h_L^+ = 1$. Let K_i be CM fields, such that $K_i^+ = L$. Suppose that $p > 2$ is unramified in K_1. Let $(d_i) = \mathrm{disc}_{K_i/L}$, $d_i \ll 0$. $(d_1, 2) = 1$. Let A_i be a principally polarized abelian variety with CM by K_i. Another generalization of Gross-Zagier can be phrased as:

Problem: *For which primes* $\mathfrak{p}$, $A_1 \cong A_2 \pmod{\mathfrak{p}}$*?*

Based on the work of Gross-Zagier it seems better to revise the question. For good primes $\mathfrak{p}$, A_i are defined over $W = W(\overline{\mathbb{F}}_p)$.

A different generalization of Gross-Zagier

Let L be a totally real field, $[L:\mathbb{Q}] = g$, $h_L^+ = 1$. Let K_i be CM fields, such that $K_i^+ = L$. Suppose that $p > 2$ is unramified in K_1. Let $(d_i) = \mathrm{disc}_{K_i/L}$, $d_i \ll 0$. $(d_1, 2) = 1$. Let A_i be a principally polarized abelian variety with CM by K_i. Another generalization of Gross-Zagier can be phrased as:

Problem: *For which primes* $\mathfrak{p}$, $A_1 \cong A_2 \pmod{\mathfrak{p}}$*?*

Based on the work of Gross-Zagier it seems better to revise the question. For good primes $\mathfrak{p}$, A_i are defined over $W = W(\overline{\mathbb{F}}_p)$.

A different generalization of Gross-Zagier

Let L be a totally real field, $[L:\mathbb{Q}] = g$, $h_L^+ = 1$. Let K_i be CM fields, such that $K_i^+ = L$. Suppose that $p > 2$ is unramified in K_1. Let $(d_i) = \mathrm{disc}_{K_i/L}$, $d_i \ll 0$. $(d_1, 2) = 1$. Let A_i be a principally polarized abelian variety with CM by K_i. Another generalization of Gross-Zagier can be phrased as:

Problem: *For which primes* $\mathfrak{p}$, $A_1 \cong A_2 \pmod{\mathfrak{p}}$*?*

Based on the work of Gross-Zagier it seems better to revise the question. For good primes $\mathfrak{p}$, A_i are defined over $W = W(\overline{\mathbb{F}}_p)$.

A different generalization of Gross-Zagier

Let L be a totally real field, $[L:\mathbb{Q}] = g$, $h_L^+ = 1$. Let K_i be CM fields, such that $K_i^+ = L$. Suppose that $p > 2$ is unramified in K_1. Let $(d_i) = \mathrm{disc}_{K_i/L}$, $d_i \ll 0$. $(d_1, 2) = 1$. Let A_i be a principally polarized abelian variety with CM by K_i. Another generalization of Gross-Zagier can be phrased as:

Problem: *For which primes* $\mathfrak{p}$, $A_1 \cong A_2 \pmod{\mathfrak{p}}$*?*

Based on the work of Gross-Zagier it seems better to revise the question. For good primes $\mathfrak{p}$, A_i are defined over $W = W(\overline{\mathbb{F}}_p)$.

What is:

$$\frac{1}{\sharp(\mathcal{O}_{K_1}^{\times}/\mathcal{O}_{L}^{\times})\cdot\sharp(\mathcal{O}_{K_2}^{\times}/\mathcal{O}_{L}^{\times})}\sum_{n=1}^{\infty}\sum_{A_1/W_n\ \textit{w. CM by } K_1}\ \sum_{A_2/W_n\ \textit{w. CM by } K_2}\sharp Isom_n(A_1,A_2)?$$

($Isom_n$ are isomorphisms between the reductions modulo (p^n), with polarization and $\mathcal{O}_L$-structure.)

Results for superspecial primes

Theorem (G. - Lauter, 2010)

It is equal to

$$\frac{1}{\sharp(\mathcal{O}_{K_1}^{\times}/\mathcal{O}_{L}^{\times})} \times \sharp \textit{ number of superspecial CM types of } K_1 \times$$

$$\sum_{n=1}^{\infty} \sum_{[\mathfrak{a}] \in CL(K_1)} \sharp S(\mathfrak{a}, \lambda_{\mathfrak{a}}, p^{n-1}).$$

We now explain the quantities appearing in this theorem.

Let us write $K_2 = L(w), \mathcal{O}_{K_2} = \mathcal{O}_L[w]$. Then $S(\mathfrak{a}, \lambda_{\mathfrak{a}}, p^{n-1})$ counts elements of trace $= Tr(w)$ and norm $= Nm(w)$ in an explicitly presented order $R(\mathfrak{a}, \lambda_{\mathfrak{a}}, p^{n-1})$ in $B_{p,\infty} \otimes_{\mathbb{Q}} L$ and the last sum can also be written using the function

$$S_2(\mathfrak{a}, x) = \sharp\{\mathfrak{b} \subseteq \mathcal{O}_K : Nm(\mathfrak{b}) = \frac{x^2 - d_1 d_2}{4p^{2n-1}}, \mathfrak{b} \sim \mathfrak{a}^2 \mathcal{A}\}.$$

We first prove that

Lemma

There is a totally negative prime element $\alpha_0 \in \mathcal{O}_L$ *such that* $(\alpha_0, 2pd_1) = 1$ *and*

$$B_{p,L} \cong \left(\frac{d_1,\, \alpha_0 p}{L} \right).$$

For $\alpha,\ \beta \in \mathcal{O}_{K_1}$ *define a symbol*

$$[\alpha, \beta] := \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \in M_2(K_1).$$

$B_{p,L} \cong \{[\alpha, \beta] \mid \alpha, \beta \in K_1\}.$

We first prove that

Lemma

There is a totally negative prime element $\alpha_0 \in \mathcal{O}_L$ *such that* $(\alpha_0, 2pd_1) = 1$ *and*

$$B_{p,L} \cong \left(\frac{d_1,\, \alpha_0 p}{L} \right).$$

For $\alpha,\ \beta \in \mathcal{O}_{K_1}$ *define a symbol*

$$[\alpha, \beta] := \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \in M_2(K_1).$$

$B_{p,L} \cong \{[\alpha, \beta] \mid \alpha, \beta \in K_1\}.$

Orders in the quaternion algebra $B_{p,L}$

Write $\alpha_0 \mathcal{O}_{K_1} = \mathcal{A} \cdot \overline{\mathcal{A}}$, and let $\mathcal{D}$ be the different of K_1/L. For each $\mathfrak{q} \mid d_1$, fix a solution $\lambda_{\mathfrak{q}}$ to

$$x^2 \equiv \alpha_0 p \mod \mathfrak{q}.$$

Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_{K_1}$. Let $\varepsilon(\mathfrak{a}, \mathfrak{q}) \in \{\pm 1\}$ be a choice of sign $\forall \mathfrak{q} \mid d_1$. Let $\lambda \in \mathcal{O}_L$ be such that

1. $\lambda \equiv \varepsilon(\mathfrak{a}, \mathfrak{q}) \lambda_{\mathfrak{q}} \mod \mathfrak{q}, \forall \mathfrak{q} \mid d_1$
2. $\lambda \mathcal{A}^{-1} \mathfrak{a}^{-1} \overline{\mathfrak{a}}$ is an integral ideal of $\mathcal{O}_{K_1}$.

Orders in the quaternion algebra $B_{p,L}$

Write $\alpha_0\mathcal{O}_{K_1} = \mathcal{A}\cdot\overline{\mathcal{A}}$, and let $\mathcal{D}$ be the different of K_1/L. For each $\mathfrak{q} \mid d_1$, fix a solution $\lambda_{\mathfrak{q}}$ to

$$x^2 \equiv \alpha_0 p \mod \mathfrak{q}.$$

Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_{K_1}$. Let $\varepsilon(\mathfrak{a},\mathfrak{q}) \in \{\pm 1\}$ be a choice of sign $\forall \mathfrak{q} \mid d_1$. Let $\lambda \in \mathcal{O}_L$ be such that

1. $\lambda \equiv \varepsilon(\mathfrak{a},\mathfrak{q})\lambda_{\mathfrak{q}} \mod \mathfrak{q}, \forall \mathfrak{q} \mid d_1$
2. $\lambda\mathcal{A}^{-1}\mathfrak{a}^{-1}\overline{\mathfrak{a}}$ is an integral ideal of $\mathcal{O}_{K_1}$.

Let $\ell \in \mathcal{O}_L$ be such that $(\ell, \alpha_0 d_1 \mathfrak{a}^{-1}\overline{\mathfrak{a}}) = 1$. Let

$$R(\mathfrak{a}, \lambda, \ell) = \{[\alpha, \beta] \mid \alpha \in \mathcal{D}^{-1}, \beta \in \mathcal{D}^{-1}\mathcal{A}^{-1}\ell\mathfrak{a}^{-1}\overline{\mathfrak{a}}, \alpha \equiv \lambda\beta \mod \mathcal{O}_{K_1}\}.$$

Lemma

1. *$R(\mathfrak{a}, \lambda, \ell)$ is an order of $B_{p,L}$, containing $\mathcal{O}_{K_1}$.*
2. *$R(\mathfrak{a}, \lambda, \ell)$ has discriminant $p \cdot \ell$.*
3. *$R(\mathfrak{a}, \lambda, \ell)$ does not depend on the choice of λ.*

Let $\ell \in \mathcal{O}_L$ be such that $(\ell, \alpha_0 d_1 \mathfrak{a}^{-1}\overline{\mathfrak{a}}) = 1$. Let

$$R(\mathfrak{a}, \lambda, \ell) = \{[\alpha, \beta] \mid \alpha \in \mathcal{D}^{-1}, \beta \in \mathcal{D}^{-1}\mathcal{A}^{-1}\ell\mathfrak{a}^{-1}\overline{\mathfrak{a}}, \alpha \equiv \lambda\beta \mod \mathcal{O}_{K_1}\}.$$

Lemma

1. *$R(\mathfrak{a}, \lambda, \ell)$ is an order of $B_{p,L}$, containing $\mathcal{O}_{K_1}$.*
2. *$R(\mathfrak{a}, \lambda, \ell)$ has discriminant $p \cdot \ell$.*
3. *$R(\mathfrak{a}, \lambda, \ell)$ does not depend on the choice of λ.*

Superspecial Orders

Recall that our goal is to describe all *superspecial* orders of $B_{p,L}$ containing $\mathcal{O}_{K_1}$. (Eichler orders of discriminant p in this case)

Theorem

Given K_1 embedded in $B_{p,L}$, the isomorphism classes of superspecial orders containing $\mathcal{O}_{K_1}$ are in bijection with the class group of K_1:

$$\mathfrak{a} \mapsto R(\mathfrak{a}, \lambda, 1).$$

(The proof is through a lot of quaternions algebra + "such orders are related by isogenies".)

Superspecial Orders

Recall that our goal is to describe all *superspecial* orders of $B_{p,L}$ containing $\mathcal{O}_{K_1}$. (Eichler orders of discriminant p in this case)

Theorem

Given K_1 embedded in $B_{p,L}$, the isomorphism classes of superspecial orders containing $\mathcal{O}_{K_1}$ are in bijection with the class group of K_1:

$$\mathfrak{a} \mapsto R(\mathfrak{a}, \lambda, 1).$$

(The proof is through a lot of quaternions algebra + "such orders are related by isogenies".)

Superspecial Orders

Recall that our goal is to describe all *superspecial* orders of $B_{p,L}$ containing $\mathcal{O}_{K_1}$. (Eichler orders of discriminant p in this case)

Theorem

Given K_1 embedded in $B_{p,L}$, the isomorphism classes of superspecial orders containing $\mathcal{O}_{K_1}$ are in bijection with the class group of K_1:

$$\mathfrak{a} \mapsto R(\mathfrak{a}, \lambda, 1).$$

(The proof is through a lot of quaternions algebra + "such orders are related by isogenies".)

Theorem

$\mathrm{End}(A_1 \pmod{p^n}) = R(\mathfrak{a}, \lambda_{\mathfrak{a}}, p^{n-1})$.

(The proof is via crystalline deformation theory.)

Theorem

$\mathrm{End}(A_1 \pmod{p^n}) = R(\mathfrak{a}, \lambda_{\mathfrak{a}}, p^{n-1})$.

(The proof is via crystalline deformation theory.)

A general result

The presence of two CM structures on $A_2 \pmod{p} \cong A_1 \pmod{p}$, implies that we have either supersingular, or superspecial reduction. We expect to prove such a result also for supersingular primes. The key ingredients are in place, already. At any rate, we have

Theorem

Any prime over which $CM(K_1)$ can intersect $CM(K_2)$ is either supersingular or superspecial and satisfies

$$p \leq 4^g \cdot \frac{disc_{K_1} disc_{K_2}}{disc_L^4}.$$

A general result

The presence of two CM structures on $A_2 \pmod{p} \cong A_1 \pmod{p}$, implies that we have either supersingular, or superspecial reduction. We expect to prove such a result also for supersingular primes. The key ingredients are in place, already. At any rate, we have

Theorem

Any prime over which $CM(K_1)$ can intersect $CM(K_2)$ is either supersingular or superspecial and satisfies

$$p \leq 4^g \cdot \frac{disc_{K_1} disc_{K_2}}{disc_L^4}.$$

Thanks!